CLAIMS

1. Architecture of an encryption circuit (1) simultaneously processing various encryption algorithms, the circuit being capable of being coupled with a host system (HS) hosted by a computing machine, characterized in that the circuit comprises:

- an input/output module (2), responsible for the data exchanges between the host system (HS) and the circuit (1) via a dedicated bus (PCI),

- an encryption module (3) coupled with the input/output module (2), in charge of the encryption and decryption operations as well as the storage of all of the circuit's sensitive information (1); and

- isolation means (4) between the input/output module (2) and the encryption module (3), making the sensitive information stored in the encryption module (3) inaccessible to the host system (HS) and ensuring the parallelism of the operations performed by the input/output module (2) and the encryption module (3).

2. Architecture according to claim 1, characterized in that the isolation means of the circuit (1) comprises a double-port memory (4) coupled between the input/output module (2) and the encryption module (3), including its own bus and simultaneously handling the exchange of data, commands and statuses between the two modules (2 and 3), and the isolation between the two modules (2 and 3).

3. Architecture according to either of claims 1 and 2, characterized in that the encryption module (3) comprises:

- a first encryption sub-module (3_1), dedicated to the processing of symmetric encryption algorithms, coupled with the bus of the dual port memory (4);

- a second encryption sub-module (3_2), dedicated to the processing of asymmetric encryption algorithms (40) coupled with the bus of the dual-port memory (4) and including a separate internal bus isolated from the bus of the dual-port memory (4); and

- a CMOS memory (11) coupled with the dual-port memory (4) via the bus of the dual-port memory containing the encryption keys.

4. Architecture according to claim 3, characterized in that the first encryption sub-module (3_1) comprises an encryption component (9) coupled with the dual-port memory (4) via the bus of the memory (4), comprising various encryption automata, respectively dedicated to the processing of symmetric encryption algorithms, and in that the second encryption sub-module (3_2) comprises at least two encryption processors (10_1 and 10_2), respectively dedicated to the processing of asymmetric encryption algorithms, coupled with the encryption module (9) via the internal bus of the second sub-module (3_2), which is isolated from the bus of the dual port memory by a bus isolator (14).

5. Architecture according to claim 4, characterized in that both processors (10_1) and 10_2) of the encryption module (3) are of the CIP type.

6. Architecture according to claim 4, characterized in that one (10_1) of the encryption processors (10_1 and 10_2) is of the CIP type, and in that the other (10_2) is of the ACE type.

7. Architecture according to claim 4, characterized in that the encryption processor (10_2) of the ACE type is produced in programmable FPGA technology.

8. Architecture according to any of claims 4 through 7, characterized in that the encryption module (9) is of the SCE type.

9. Architecture according to claim 8, characterized in that the encryption module (9) is produced in programmable FPGA technology.

10. Architecture according to any of claims 3 through 9, characterized in that the second encryption sub-module (3_2) also comprises a flash memory PROM (12) and an SRAM memory (13) coupled with the internal bus of the sub-module (3_2).

11. Architecture according to any of claims 3 through 10, characterized in that the CMOS memory (11) is protected by security mechanisms (15) that trigger the reset mechanism of the CMOS memory (11) in case of an alarm.

12. Architecture according to any of claims 1 through 11, characterized in that the input/output module (2) comprises:

- a microcontroller (6) comprising an input/output processor (6_1) and a PCI interface (6_2) integrating DMA channels responsible for executing the data transfers between the host system (HS) and the circuit (1);

- a flash memory (7) containing the code of the input/output processor (6_1); and

- an SRAM memory (8) that receives a copy of the contents of the flash memory (7) at the startup of the input/output processor (6_1).

13. Architecture according to any of the preceding claims, comprising a serial link (SL) that makes it possible to input basic keys through a secure path independent of the PCI bus, characterized in that the link is controlled by the encryption module (3).

14. Architecture according to claim 13, characterized in that the serial link (SL) allows the downloading of proprietary algorithms into the first encryption sub-module (3_1).

ADD A27